明　細　書

発明の名称 ：

アクセス制御装置、プログラム及びアクセス制御システム

技術分野

[0001] 本発明は、アクセス制御装置、プログラム及びアクセス制御システムに関する。

背景技術

[0002] 暗号化された電子ファイルの復号化に必要な復号用パスワードを管理する管理サーバを用いて、安全かつ簡単に電子ファイルを送信する方法が知られている（例えば、特許文献１参照）。

特許文献１　特開２０１０－１５４４１９号公報

発明の概要

発明が解決しようとする課題

[0003] 電子ファイルのアクセスが許可または禁止されているソフトウエアによる電子ファイルへアクセスをアクセス制御情報に基づいて制限することができないという課題があった。

課題を解決するための手段

[0004] 第１の態様においては、アクセス制御装置は、電子ファイルのアクセスが許可または禁止されているソフトウエアが予め定められたアクセス制御情報に基づいて、電子ファイルへアクセスすることを制限する制御部を備える。

[0005] 第２の態様においては、プログラムは、コンピュータを上記のアクセス制御装置として機能させる。

[0006] 第３の態様においては、アクセス制御システムは、上記のアクセス制御装置と、アクセス制御装置の外部に設けられ、予め定められたアクセス制御情報及び予め定められたアクセス制御情報に基づく判断結果の少なくとも一方を、アクセス制御装置に提供する管理装置とを備える。

[0007] なお、上記の発明の概要は、本発明の特徴の全てを列挙したものではない

。また、これらの特徴群のサブコンビネーションもまた、発明となりうる。

図面の簡単な説明

[0008] [図1]アクセス制御システム１００の一例を通信ネットワーク９０とともに示す。

[図2]ユーザ装置１３０の機能ブロック構成の一例を模式的に示す。

[図3]許可条件に用いられるパラメータの一例をテーブル形式で示す。

[図4]拒否条件に用いられるパラメータの一例をテーブル形式で示す。

[図5]拒否条件に用いられるパラメータの一例をテーブル形式で示す。

[図6]ユーザ装置１３０における処理フローの一例を示す。

[図7]ユーザ装置１３０におけるアクセス処理に関する処理フローの一例を示す。

発明を実施するための形態

[0009] 以下、発明の実施の形態を通じて本発明を説明するが、以下の実施形態は請求の範囲にかかる発明を限定するものではない。また、実施形態の中で説明されている特徴の組み合わせの全てが発明の解決手段に必須であるとは限らない。

[0010] 図１は、アクセス制御システム１００の一例を通信ネットワーク９０とともに示す。アクセス制御システム１００は、電子ファイル等のデータに対するＩＲＭ（Ｉｎｆｏｒｍａｔｉｏｎ Ｒｉｇｈｔｓ Ｍａｎａｇｅｍｅｎｔ）機能を提供する。アクセス制御システム１００は、ユーザ装置１１０と、管理サーバ１２０と、ユーザ装置１３０とを備える。通信ネットワーク９０は、例えばインターネットを含む。通信ネットワーク９０は、固定網及び移動体通信網を含んでよい。

[0011] 管理サーバ１２０は、ユーザ装置１１０の外部に設けられる。管理サーバ１２０は、ユーザ装置１３０の外部に設けられる。ユーザ装置１１０、管理サーバ１２０及びユーザ装置１３０は、通信ネットワーク９０を介して情報を送受信する。ユーザ装置１１０は、例えば、パーソナルコンピュータ、携帯電話端末、携帯情報端末等であってよい。ユーザ装置１３０は、例えば、

パーソナルコンピュータ、携帯電話端末、携帯情報端末等であってよい。

[0012] ユーザ装置１３０は、アクセス制御情報に基づいて電子ファイルへのアクセスを制限するアクセス制御装置の一例である。ユーザ装置１３０には、アクセス制御情報に基づいて電子ファイルへのアクセスを制限するための制御ソフトウエア１０がインストールされる。

[0013] 管理サーバ１２０は、コンピュータによって実現される。管理サーバ１２０は、アクセス制御情報をユーザ装置１３０に提供する管理装置の一例である。

[0014] 本実施形態において、ユーザ１８０は、電子ファイル２０を作成する作成者である。ユーザ１８０は、ユーザ装置１１０を用いて電子ファイルを作成する。ユーザ１９０は、ユーザ１８０が作成した電子ファイル２０のデータにアクセスするアクセス者である。例えば、ユーザ１９０は、ユーザ装置１３０を用いて、電子ファイル２０のデータを閲覧する。

[0015] ユーザ装置１１０は、ユーザ１８０の指示に基づいて、電子ファイル２０を作成する。また、ユーザ装置１１０は、ユーザ１８０の指示に基づいて、電子ファイル２０のデータに対するアクセス制限を設定する。例えば、ユーザ１８０は、電子ファイル２０のデータにアクセスすることが許可されるアクセス許可者を指定する。また、ユーザ１８０は、電子ファイル２０のデータに対してアクセス許可者が行うことが許可される操作内容または禁止される操作内容を指定する。電子ファイル２０のデータに対して許可または禁止される操作内容としては、閲覧、印刷、透かし付き印刷、編集、保存、クリップボード等の記憶領域へのデータのコピー、表示画面のキャプチャ等を例示することができる。ユーザ装置１１０は、アクセス許可者のユーザ識別情報を含む許可者情報と、許可または禁止される操作内容を識別する操作情報とを含む操作制限情報を生成する。

[0016] ユーザ装置１１０は、パスフレーズ６０を用いて電子ファイル２０を暗号化することにより、暗号化ファイル３０を生成する。パスフレーズ６０は、ユーザ装置１１０が生成してよく、ユーザ１８０が指定してもよい。パスフ

レーズは、パスワードと称される場合がある。暗号化ファイル３０には、電子ファイル２０の拡張子を示す情報と、電子ファイル２０のファイル識別情報を特定する情報とを含む。ユーザ装置１１０は、電子ファイル２０を識別するファイル識別情報と、操作制限情報と、パスフレーズ６０とを含むファイル管理情報を、管理サーバ１２０に送信する。管理サーバ１２０は、ユーザ装置１１０から受信したファイル管理情報を格納する。

[0017] ユーザ装置１１０は、暗号化ファイル３０のデータをユーザ１９０に提供する。例えば、ユーザ装置１１０は、暗号化ファイル３０を添付した電子メール７０を、通信ネットワーク９０を介してユーザ１９０宛に送信する。また、ユーザ装置１１０は、不揮発性の記録メディア８０に暗号化ファイル３０のデータを記録する。この場合、記録メディア８０がユーザ１９０に渡されることにより、暗号化ファイル３０のデータがユーザ１９０に提供される。また、ユーザ装置１１０は、ユーザ装置１１０及びユーザ装置１３０がアクセスできる共有ストレージに暗号化ファイル３０のデータを格納してよい。

[0018] ユーザ装置１３０は、ユーザ装置１１０から提供された暗号化ファイル３０のデータを取得する。ユーザ装置１３０は、暗号化ファイル３０が添付された電子メールを受信することにより、暗号化ファイル３０のデータを取得する。また、ユーザ装置１３０は、記録メディア８０から暗号化ファイル３０を読み込むことにより、暗号化ファイル３０のデータを取得する。ユーザ装置１３０は、上述した共有ストレージから暗号化ファイル３０のデータを取得することにより、暗号化ファイル３０のデータを取得する。

[0019] なお、ユーザ装置１３０が取得した暗号化ファイル３０のデータは、ユーザ装置１１０で作成された暗号化ファイル３０のデータと同一である。そのため、本実施形態を分かり易く説明することを目的として、ユーザ装置１３０において扱われる暗号化ファイル３０のデータのことを、「暗号化ファイル３０」と呼ぶ場合がある。

[0020] ユーザ装置１３０は、ユーザ１９０の指示に応じて、暗号化ファイル３０

を開く。このとき、ユーザ装置１３０は、ソフトウエアの実行設定及びソフトウエアの動作状態の少なくとも一方に基づいて、電子ファイル２０のデータに対するアクセスが許可される状態にあるか否かを判断する。例えば、ユーザ装置１３０は、暗号化ファイル３０を復号化して得られる電子ファイルの閲覧に用いられる閲覧ソフトウエアが、予め定められた許可条件を満たすソフトウエアである場合に、アクセスが許可される状態にあると判断する。また、ユーザ装置１３０は、予め定められた拒否条件を満たすソフトウエアがユーザ装置１３０で動作していない場合に、アクセスが許可される状態にあると判断する。なお、許可条件及び拒否条件は、アクセス制御情報の一例である。

[0021] 本実施形態の説明において、予め定められた許可条件を満たすソフトウエアを、許可ソフトウエアと呼ぶ場合がある。また、予め定められた拒否条件を満たすソフトウエアを、拒否ソフトウエアと呼ぶ場合がある。許可ソフトウエアとしては、制御ソフトウエア１０が上述した閲覧等の操作を制御することが可能なソフトウエアが指定される。例えば、制御ソフトウエア１０によってＩＲＭ機能を管理できる許可ソフトウエアが、許可ソフトウエアとして指定される。これに対し、拒否ソフトウエアとしては、上述した閲覧等の操作を、制御ソフトウエア１０が制御できない可能性があるソフトウエアが指定される。また、表示画面のキャプチャ動作やクリップボード等へのデータのコピー動作等のデータアクセス動作を行うソフトウエアを、拒否ソフトウエアとして指定する。ユーザ装置１３０は、電子ファイル２０のデータに対するアクセスが許可される状態にあると判断すると、ユーザ１９０を識別するユーザ識別情報及びファイル識別情報とともに、管理サーバ１２０にパスフレーズ６０及び操作制限情報を要求する。

[0022] 管理サーバ１２０は、ユーザ装置１３０から取得したユーザ識別情報及びファイル識別情報と、ファイル管理情報に含まれる許可者情報とに基づいて、ユーザ１９０が電子ファイル２０のデータに対するアクセス許可者に含まれるか否かを判断する。管理サーバ１２０は、ユーザ１９０がアクセス許可

者に含まれると判断した場合に、パスフレーズ６０及び操作制限情報をユーザ装置１３０に送信する。

[0023] ユーザ装置１３０は、管理サーバ１２０からパスフレーズ６０及び操作制限情報を受信すると、受信したパスフレーズ６０を用いて暗号化ファイル３０を復号化して、復号化ファイル５０を生成する。ユーザ装置１３０は、制御ソフトウエア１０の制御に従って、閲覧ソフトウエアを用いて復号化ファイル５０を開き、管理サーバ１２０から受信した操作制限情報に基づいて復号化ファイル５０にアクセスする。これにより、ユーザ装置１３０は、元の電子ファイル２０のデータと同じデータにアクセスすることができる。

[0024] 制御ソフトウエア１０による係る制御により、制御ソフトウエア１０で制御できない可能性がある閲覧ソフトウエアで復号化ファイル５０が開かれることを抑制できる。また、制御ソフトウエア１０で制御できないソフトウエアや閲覧ソフトウエア以外のソフトウエアによって、復号化ファイル５０のデータがアクセスされることを抑制できる。

[0025] 図２は、ユーザ装置１３０の機能ブロック構成の一例を模式的に示す。ユーザ装置１３０は、制御部２００と、送受信部２０２と、格納部２０４とを有する。制御部２００は、例えば、ＭＰＵ等のプロセッサで実現される。送受信部２０２は、ネットワークインタフェース等の通信モジュール等で実現される。なお、送受信部２０２は、通信ネットワーク９０を通じた通信を担う。具体的には、送受信部２０２は、管理サーバ１２０に、ユーザ識別情報およびファイル識別情報を送信する。送受信部２０２は、管理サーバ１２０から、操作制限情報、パスフレーズ及びアクセス制御情報を取得する。格納部２０４は、ハードディスク等の不揮発性の記憶媒体、ＲＡＭ等の揮発性の記憶媒体で実現される。格納部２０４は、送受信部２０２が受信したアクセス制御情報を格納する。

[0026] 制御部２００は、判断部２１０と、動作状態取得部２２０と、ソフトウエア特定部２３０と、動作処理部２４０と、アクセス処理部２５０とを有する。ユーザ装置１３０は、制御ソフトウエア１０の制御に従って制御部２００

が動作することにより、判断部２１０、動作状態取得部２２０、ソフトウエア特定部２３０、動作処理部２４０及びアクセス処理部２５０として機能する。

[0027] 制御部２００は、電子ファイルのアクセスが許可または禁止されているソフトウエアが電子ファイルへアクセスすることを予め定められたアクセス制御情報に基づいて制限する。アクセス制御情報は、電子ファイルへのアクセスに用いることが許可されるソフトウエアが満たすべき許可条件を含む。また、アクセス制御情報は、電子ファイルへのアクセスが禁止されるソフトウエアが満たすべき予め定められた拒否条件を含む。本実施形態において、許可条件及び拒否条件は、管理サーバ１２０から提供される。格納部２０４は、管理サーバ１２０から受信した許可条件及び拒否条件を格納する。

[0028] 制御部２００は、電子ファイルのアクセスに用いるべきソフトウエアが許可条件を満たす場合に、許可条件を満たすソフトウエアによるアクセスを許可する。具体的には、ソフトウエア特定部２３０は、電子ファイルのアクセスに用いるべきソフトウエアを特定する。例えば、ソフトウエア特定部２３０は、電子ファイルの拡張子に基づいて、電子ファイルのアクセスに用いるべきソフトウエアを特定する。判断部２１０は、ソフトウエア特定部２３０が特定したソフトウエアが、格納部２０４が格納している許可条件を満たすか否かを判断する。動作処理部２４０は、ソフトウエア特定部２３０が特定したソフトウエアが許可条件を満たすと判断部２１０が判断した場合に、許可条件を満たすソフトウエアによるアクセスを開始させる。

[0029] 一例として、許可条件は、アクセスが許可されるべきソフトウエアの名前である許可ソフトウエア名に基づく判断条件を含む。この場合、ソフトウエア特定部２３０は、電子ファイルのアクセスに用いるべきソフトウエアの名前を特定する。判断部２１０は、ソフトウエア特定部２３０が特定したソフトウエアの名前に一致するソフトウエア名が、許可条件で用いられる許可ソフトウエア名の中に含まれる場合に、ソフトウエア特定部２３０が特定したソフトウエアが許可条件を満たすと判断する。なお、ソフトウエアの名前は

、ソフトウエアを識別するためのソフトウエア識別情報の一例である。

[0030] 制御部２００は、拒否条件を満たすソフトウエアによるアクセスを制限する。また、制御部２００は、拒否条件を満たすソフトウエアが動作している場合に、許可条件を満たすソフトウエアによる電子ファイルへのアクセスを制限する。

[0031] 例えば、制御部２００は、許可条件を満たすソフトウエアが電子ファイルへのアクセスを開始する前に、拒否条件を満たすソフトウエアが動作しているか否かを判断する。制御部２００は、拒否条件を満たすソフトウエアが動作していると判断した場合に、許可条件を満たすソフトウエアが電子ファイルへのアクセスを開始することを禁止する。また、制御部２００は、許可条件を満たすソフトウエアが電子ファイルへのアクセスを開始した後に、拒否条件を満たすソフトウエアの動作が検出された場合に、拒否条件を満たすソフトウエアの動作を制限する。

[0032] 具体的には、動作状態取得部２２０は、許可条件を満たすソフトウエアに電子ファイルへのアクセスを開始させる前に、ユーザ装置１３０で動作しているソフトウエアを識別する一覧情報を取得する。

[0033] 一例として、拒否条件は、アクセスが拒否されるべきソフトウエアの名前に基づく判断条件を含む。例えば、拒否条件は、拒否するべきソフトウエアを実行した場合に生成されるプロセスの名前である禁止プロセス名に基づく判断条件を含む。この場合、動作状態取得部２２０は、現在実行中のプロセスの名前を取得する。

[0034] 判断部２１０は、動作状態取得部２２０が取得したプロセスの名前が、禁止条件で用いられる１以上の禁止プロセス名の中に含まれる場合に、拒否条件を満たすソフトウエアが動作していると判断する。この場合、動作処理部２４０は、許可条件を満たすソフトウエアに電子ファイルへのアクセスを開始させない。一方、判断部２１０は、動作状態取得部２２０が取得したプロセスの名前が、禁止条件で用いられる１以上の禁止プロセス名の中に含まれない場合に、拒否条件を満たすソフトウエアが動作していないと判断する。

この場合、動作処理部２４０は、許可条件を満たすソフトウエアに電子ファイルへのアクセスを開始させる。

[0035] また、制御部２００は、許可条件を満たすソフトウエアが電子ファイルへのアクセスを開始した後に、拒否条件を満たすソフトウエアの動作が検出された場合に、拒否条件を満たすソフトウエアの動作を制限する。具体的には、動作状態取得部２２０は、電子ファイルのアクセス中においても、実行中のプロセスの名前を定期的に取得する。そして、判断部２１０は、動作状態取得部２２０が取得したプロセスの名前の中から、禁止条件で用いられる１以上の禁止プロセス名のいずれかに一致する名前のプロセスが検出された場合に、動作処理部２４０は、検出されたプロセスの動作を停止させる。

[0036] なお、拒否条件は、アクセスが禁止されるべきソフトウエアが行う動作内容に関する動作条件を含んでよい。例えば、拒否条件は、予め定められた禁止されたＡＰＩをコールするソフトウエアであるか否かに基づく判断条件を含んでよい。例えば、拒否条件は、予め定められた禁止されたＡＰＩをコールするコードをソフトウエアが含むか否かの判断条件を含んでよい。この場合、判断部２１０は、動作状態取得部２２０が取得したプロセスの実行ファイルに、予め定められた禁止されたＡＰＩをコールするコードが含まれる場合に、拒否条件を満たすソフトウエアが動作していると判断する。

[0037] なお、アクセス処理部２５０は、暗号化された電子ファイルの復号化に用いるパスフレーズを管理サーバ１２０から取得して、取得したパスフレーズを用いて、暗号化された電子ファイルを復号化する。判断部２１０は、暗号化された電子ファイルをアクセス処理部２５０が復号化する前に、復号化により得られる電子ファイルである復号化ファイルへのアクセスを許可するか否かを、アクセス制御情報に基づいて判断する。アクセス処理部２５０は、判断部２１０が復号化ファイルへのアクセスを許可すると判断した場合に、管理サーバ１２０からパスフレーズを取得する。そして、アクセス処理部２５０は、暗号化した電子ファイルを、管理サーバ１２０から取得したパスフレーズを用いて復号化することにより復号化ファイルを生成する。そして、

動作処理部２４０は、生成された復号化ファイルを、許可条件を満たすソフトウエアでアクセスさせる。

[0038] なお、ユーザ装置１３０は、管理サーバ１２０にアクセスして、管理サーバ１２０から許可条件及び拒否条件を含むアクセス制御情報を取得する。ユーザ装置１３０は、定期的に管理サーバ１２０にアクセスしてアクセス制御情報を取得してよい。ユーザ装置１３０は、予め定められたイベントが生じた場合に、管理サーバ１２０にアクセスしてアクセス制御情報を取得してよい。例えば、管理サーバ１２０から通知された場合に、管理サーバ１２０にアクセス制御情報を取得すべき旨が通知された場合に、管理サーバ１２０からアクセス制御情報を取得してよい。格納部２０４は、管理サーバ１２０から取得されたアクセス制御情報を格納する。格納部２０４が格納するアクセス制御情報は、管理サーバ１２０から新たに取得されたアクセス制御情報によって更新される。なお、管理サーバ１２０のアクセス制御条件は、管理サーバ１２０の管理者によって更新される。管理サーバ１２０の管理者によって、最新の情報に更新される。

[0039] 図３は、許可条件に用いられるパラメータの一例をテーブル形式で示す。格納部２０４は、許可条件に用いられるパラメータとして、ファイルの拡張子と、許可ソフトウエアのソフトウエア名と、許可種別とを対応づけて格納する。判断部２１０は、図３に示すパラメータを判断基準として用いた許可条件に基づいて、閲覧ソフトウエアが許可ソフトウエアであるか否かを判断する。

[0040] 「拡張子」は、ファイルの種類を識別する情報の一例である。なお、本実施形態の説明において、ファイルの拡張子のことを単に「拡張子」と呼ぶ場合がある。拡張子は、ユーザ装置１３０で動作するオペレーティングシステム等の基本ソフトウエアが、ファイルを開くのに用いるソフトウエアを決定するために用いる場合がある。基本ソフトウエアの設定情報には、ファイルを開くのに用いるソフトウエアと拡張子とを関連づける関連付け情報が含まれる。したがって、拡張子は、ファイルを開くのに用いるソフトウエアとフ

ァイルとの関連付けに用いられる関連付け情報の一例でもある。

[0041] 「ソフトウエア名」には、許可ソフトウエアの名前が格納される。「許可種別」には、基本ソフトウエアの設定を優先するべきであるか否かを示す情報が格納される。「許可種別」には、「基本ソフトウエア優先」を示す値及び「制御ソフトウエア優先」を示す値の何れかが格納される。

[0042] 「基本ソフトウエア優先」は、基本ソフトウエアの設定情報に基づく関連付けを優先することを示す。具体的には、ソフトウエア特定部２３０は、暗号化ファイル３０を開く場合に、暗号化ファイル３０の復号化により得られる復号化ファイルの拡張子と、基本ソフトウエアの設定情報に含まれる関連付け情報とに基づいて、復号化ファイルを開くのに用いるソフトウエアを特定する。判断部２１０は、ソフトウエア特定部２３０が特定したソフトウエアの名前が、復号化ファイルの拡張子に対応づけられているソフトウエアの名前のいずれかに一致する場合に、ソフトウエア特定部２３０が特定したソフトウエアを用いて、復号化ファイルのデータに対するアクセスを許可すると判断する。なお、「基本ソフトウエア優先」に対応づけられる許可ソフトウエアの数は、１以上であってよい。「基本ソフトウエア優先」に対応づけられる許可ソフトウエアの数は２以上であってよい。

[0043] 「制御ソフトウエア優先」は、基本ソフトウエアの設定にかかわらず、許可条件で対応づけられた特定のソフトウエアを用いて開くことを示す。例えば、暗号化ファイルの拡張子が”ｊｐｇ”である場合、判断部２１０は、”ＡＡＰａｉｎｔ”の名前のソフトウエアを用いて、復号化ファイルのデータに対するアクセスを許可すると判断する。「制御ソフトウエア優先」に対応づけられる許可ソフトウエアの数は、１であってよい。この場合、判断部２１０は、「制御ソフトウエア優先」に対応づけられている１つの許可ソフトウエアがユーザ装置１３０にインストールされていることを条件として、当該許可ソフトウエアを用いて復号化ファイルのデータに対してアクセスすることを許可すると判断する。

[0044] なお、「制御ソフトウエア優先」に対応づけられる許可ソフトウエアの数

は２以上であってよい。この場合、判断部２１０は、「制御ソフトウエア優先」に対応づけられている２以上の許可ソフトウエアのうち、ユーザ装置１３０にインストールされている１以上の許可ソフトウエアを特定して、特定した１以上の許可ソフトウエアを用いて復号化ファイルのデータに対してアクセスすることを許可すると判断してよい。「制御ソフトウエア優先」に対応づけられている２以上の許可ソフトウエアがユーザ装置１３０にインストールされている場合、判断部２１０は、「制御ソフトウエア優先」に対応づけられている２以上の許可ソフトウエアのうち１つの許可ソフトウエアを用いて復号化ファイルのデータに対してアクセスすることを許可すると判断する。このとき、判断部２１０は、「制御ソフトウエア優先」に対応づけられている２以上の許可ソフトウエアの中から、復号化ファイルのデータに対してアクセスすることを許可する１つの許可ソフトウエアを、予め定められた選択条件に基づいて選択してよい。例えば格納部２０４は、選択条件として、２以上の許可ソフトウエアに対応づけてそれぞれの許可ソフトウエアを選択する優先順位を格納している。判断部２１０は、格納部２０４が格納している選択条件に基づき、ユーザ装置１３０にインストールされている２以上の許可ソフトウエアの中で、優先順位が最も高い１つの許可ソフトウエアを、復号化ファイルのデータに対してアクセスすることを許可する許可ソフトウエアとして選択する。このようにして、１つの閲覧ソフトウエアが特定される。なお、選択条件は、アクセス制御情報の一部として、管理サーバ１２０からユーザ装置１３０に提供されてよい。

[0045] なお、許可ソフトウエアの名前は、許可ソフトウエアを特定するための許可ソフトウエア特定情報の一例である。許可ソフトウエア特定情報には、許可ソフトウエアの名前及び許可ソフトウエアのバージョンを示す情報を含んでよい。また、許可ソフトウエア特定情報には、許可ソフトウエアの名前に代えてまたは許可ソフトウエアの名前に加えて、許可ソフトウエアの実行ファイルの一部をハッシュ化したハッシュ値等を含んでよい。

[0046] 図４は、拒否条件に用いられるパラメータの一例をテーブル形式で示す。

格納部２０４は、拒否条件に用いられるパラメータの一部として、プロセス名を格納する。判断部２１０は、図４に示すパラメータを判断基準として用いた拒否条件に基づいて、拒否ソフトウエアの動作状態を判断する。

[0047] 「プロセス名」には、拒否ソフトウエアを実行した場合に生成されるプロセスの名前が格納される。プロセスは、拒否ソフトウエアの実行ファイルを実行した場合に基本ソフトウエアが割り当てる実行単位である。プロセスと実行ファイルとは互いに関連する。判断部２１０は、格納部２０４が格納しているパラメータに基づく拒否条件に基づいて、復号化ファイルのデータに対するアクセスを許可するか否かを判断する。

[0048] 例えば、動作状態取得部２２０は、暗号化ファイル３０を開く場合に、基本ソフトウエアから現在実行中のプロセスの名前を取得する。判断部２１０は、動作状態取得部２２０が取得したプロセスの名前が、「プロセス名」に格納されているプロセスの名前のいずれかに一致する場合に、復号化後の電子ファイルのデータに対するアクセスを拒否すると判断する。

[0049] プロセス名の拒否条件には、プロセス名の文字列に対する部分一致条件が含まれてよい。例えば、図４におけるパラメータ”＊ｃａｐｔｕｒｅ＊”は、”ｃａｐｔｕｒｅ”の前に０個以上の文字を含み、”ｃａｐｔｕｒｅ”の後に０個以上の文字を含む文字列で構成されるプログラム名が、拒否条件に適合すると判断される。このように、プロセス名に基づく拒否条件によって、いわゆる商用ソフトウエアに限らず、復号化ファイルのデータにアクセスする可能性があるソフトウエアを、拒否ソフトウエアとして判断することができる場合がある。

[0050] 図５は、格納部２０４が格納する拒否条件のパラメータの一例をテーブル形式で示す。格納部２０４は、拒否条件のパラメータの一部として、ＡＰＩ名を格納する。判断部２１０は、図５に示すパラメータを判断基準として用いた拒否条件に基づいて、拒否ソフトウエアの動作状態を判断する。

[0051] 「ＡＰＩ名」には、拒否ソフトウエアを実行した場合に呼び出されるＡＰＩ（アプリケーションプログラミングインタフェース）の名前が格納される

。ＡＰＩには、基本ソフトウエアが外部のソフトウエアに提供するＡＰＩやシステムコール等が含まれる。ＡＰＩには、ライブラリとして提供される関数等を含む、ソフトウエアインタフェースの一例である。なお、ソフトウエアインタフェースには、基本ソフトウエアの一部として提供されるライブラリが提供するソフトウエアインタフェース以外にも、サードパーティが提供するライブラリが提供するソフトウエアインタフェースや、個人が自作したライブラリが提供するソフトウエアインタフェース等を含む。

[0052] 判断部２１０は、ＡＰＩに関するパラメータに基づく拒否条件に基づいて、暗号化ファイル３０を復号化した後の電子ファイルのデータに対するアクセスを許可するか否かを判断する。例えば、判断部２１０は、動作状態取得部２２０が取得したプロセスの実行ファイルが、「ＡＰＩ名」に格納されている名前に適合する名前のＡＰＩを呼ぶ場合に、復号化ファイルのデータに対するアクセスを拒否すると判断する。例えば、判断部２１０は、動作状態取得部２２０が取得したプロセスの実行ファイルに、「ＡＰＩ名」に格納されているＡＰＩをコールするコードが含まれている場合に、復号ファイルのデータに対するアクセスを拒否すると判断する。

[0053] なお、ＡＰＩ名の拒否条件には、ＡＰＩ名の文字列に対する部分一致条件が含まれてよい。例えば、図５におけるパラメータ”＊Ｃｌｉｐｂｏａｒｄ＊”は、”Ｃｌｉｐｂｏａｒｄ”の前に０個以上の文字を含み、”Ｃｌｉｐｂｏａｒｄ”の後に０個以上の文字を含む文字列で構成されるＡＰＩ名のＡＰＩをコールするソフトウエアが、拒否条件に適合すると判断される。このように、ＡＰＩ名に基づく拒否条件によって、いわゆる商用ソフトウエアに限らず、復号化ファイルのデータにアクセスする可能性があるソフトウエアを、拒否ソフトウエアとして判断することができる場合がある。

[0054] なお、上述したプロセスの名前及びＡＰＩの名前は、拒否ソフトウエアを特定するための拒否ソフトウエア特定情報の一例である。拒否ソフトウエア特定情報は、許可ソフトウエアの実行ファイルの少なくとも一部をハッシュ化して得られたハッシュ値を含んでよい。判断部２１０は、実行中のプロセ

スに関する実行ファイルの予め定められた部分をハッシュ値して得られたハッシュ値が、拒否ソフトウエア特定情報として格納されたハッシュ値のいずれかに一致した場合に、復号化ファイルのデータに対するアクセスを拒否すると判断してよい。

[0055] また、拒否ソフトウエア特定情報は、ソフトウエアの実行ファイルの格納場所を示す情報を含んでよい。例えば、判断部２１０は、ソフトウエアの実行ファイルが格納されているディレクトリが、予め定められたディレクトリの配下にない場合に、復号化ファイルのデータに対するアクセスを拒否すると判断してよい。例えば、判断部２１０は、動作状態取得部２２０が取得したプロセスの実行ファイルが格納されているディレクトリが、ソフトウエアがインストールされる規定のドライブ直下の”Ｐｒｏｇｒａｍ　Ｆｉｌｅｓ”の配下にない場合に、復号化ファイルのデータに対するアクセスを拒否すると判断してよい。

[0056] 図６は、ユーザ装置１３０が実行する処理フローの一例を示す。図６の処理フローは、暗号化ファイル３０を開くことをユーザ１９０から指示された場合に、開始される。例えば、図６の処理フローは、暗号化ファイル３０に関連付けられたアイコンがダブルクリックされた場合に、開始される。

[0057] ステップＳ６０２において、制御ソフトウエア１０の実行が開始される。例えば、制御ソフトウエア１０は、基本ソフトウエアによって起動される。上述したように、基本ソフトウエアの設定情報には、ソフトウエアと拡張子との関連付け情報が含まれる。基本ソフトウエアの関連付け情報によって、暗号化ファイルの拡張子にはアクセス制御ソフトウエア１０が関連付けられている。このため、例えば暗号化ファイル３０に関連付けられたアイコンがダブルクリックされた場合、基本ソフトウエアは、オープン対象のファイルとして暗号化ファイル３０を指定して、制御ソフトウエア１０の実行ファイルが起動される。

[0058] ステップＳ６０４において、ソフトウエア特定部２３０は、暗号化ファイル３０に基づいて、暗号化前の電子ファイル２０の拡張子を特定する。例え

ば、ユーザ装置１１０において電子ファイル２０が暗号化される場合に、ユーザ装置１１０は暗号化前の電子ファイル２０の拡張子を示す拡張子情報を含めて暗号化ファイル３０を生成する。ソフトウエア特定部２３０は、暗号化ファイル３０から拡張子情報を抽出することにより、暗号化前の電子ファイル２０の拡張子を特定する。なお、暗号化前の電子ファイル２０の拡張子は、復号化ファイル５０の拡張子と一致する。

[0059] ステップＳ６０６において、ソフトウエア特定部２３０は、ステップＳ６０４で特定した拡張子に基づいて、基本ソフトウエアの設定情報に基づく関連付けを優先するか、制御ソフトウエア１０による設定情報を優先するかを判断する。例えば、ソフトウエア特定部２３０は、ステップＳ６０４で特定した拡張子に対応づけて許可条件の許可種別に格納されている情報が「基本ソフトウエア優先」の情報である場合に、基本ソフトウエアの設定情報に基づく関連付けを優先すると判断する。一方、ソフトウエア特定部２３０は、ステップＳ６０４で特定した拡張子に対応づけて許可条件の許可種別に格納されている情報が「制御ソフトウエア優先」の情報である場合に、制御ソフトウエア１０の情報に基づく関連付けを優先すると判断する。

[0060] ステップＳ６０６において、ソフトウエア特定部２３０が基本ソフトウエアの設定情報に基づく関連付けを優先すると判断した場合、ステップＳ６０８に進む。ソフトウエア特定部２３０が制御ソフトウエアの設定情報に基づく関連付けを優先すると判断した場合、ステップＳ６２２に進む。ステップＳ６２２では、ステップＳ６０４で特定した拡張子に対応づけて「ソフトウエア名」に格納されている名前で識別されるソフトウエアを、閲覧ソフトウエアとして特定する。ステップＳ６２２の処理が完了すると、ステップＳ６１２に進む。

[0061] ステップＳ６０８において、ソフトウエア特定部２３０は、ステップＳ６０４で特定した拡張子及び基本ソフトウエアの設定情報に基づき、閲覧ソフトウエアを特定する。上述したように、ソフトウエア特定部２３０は、基本ソフトウエアの設定情報に含まれる関連付け情報に基づいて、ステップＳ６

０４で特定した拡張子を開くのに用いるソフトウエアを特定して、特定したソフトウエアを閲覧ソフトウエアとして決定する。

[0062] ステップＳ６１０において、判断部２１０は、ステップＳ６０８で特定した閲覧ソフトウエアを用いて復号化ファイルのデータにアクセスすることが許可されるか否かを判断する。具体的には、判断部２１０は、ステップＳ６０４で特定した拡張子に対応づけて許可条件のソフトウエア名に格納されているソフトウエアの名前の中に、ステップＳ６０８で特定したソフトウエアの名前に一致するものが存在する場合に、ステップＳ６０８で特定した閲覧ソフトウエアを用いて復号化ファイルのデータにアクセスすることが許可されると判断する。

[0063] ステップＳ６１０において、ステップＳ６０８で特定した閲覧ソフトウエアを用いて復号化ファイルのデータにアクセスすることが許可されると判断した場合、ステップＳ６１２に進み、ステップＳ６０８で特定した閲覧ソフトウエアを用いて復号化ファイルのデータにアクセスすることが許可されないと判断した場合、ステップＳ６３２に進む。ステップＳ６３２では、関連付けされたソフトウエアでは復号化ファイルのデータへのアクセスが拒否されている旨をユーザ１９０に通知して、制御ソフトウエア１０の動作を終了する。

[0064] ステップＳ６１２において、動作状態取得部２２０は、現在実行中のプロセスの名前を取得する。具体的には、動作状態取得部２２０は、基本ソフトウエアが提供するＡＰＩを通じて、現在実行中のプロセスの名前を取得する。

[0065] ステップＳ６１４において、判断部２１０は、現在実行中のプロセスに基づいて、閲覧ソフトウエアによる復号化ファイルへのアクセスを許可するか否かを判断する。具体的な判断処理として、判断部２１０は、ステップＳ６１２で取得したプロセスの名前のうちの少なくとも一つのプロセスの名前が、拒否条件のプロセス名に格納されているプロセスの名前のいずれかに一致する場合に、閲覧ソフトウエアによる復号化ファイルへのアクセスを拒否す

ると判断する。また、判断部２１０は、ステップＳ６１２で取得したプロセスの実行ファイルに、拒否条件の「ＡＰＩ名」に格納されている名前に適合する名前のＡＰＩをコールするコードが含まれている場合に、閲覧ソフトウエアによる復号化ファイルへのアクセスを拒否すると判断する。

[0066] ステップＳ６１４において、復号化後の電子ファイルのデータへのアクセスを拒否すると判断した場合、ステップＳ６４２に進み、復号化後の電子ファイルのデータに対するアクセスを拒否しないと判断した場合、ステップＳ６１６に進む。ステップＳ６４２では、復号化ファイルのデータにアクセスできない旨をユーザ１９０に通知して、制御ソフトウエア１０の動作を終了する。このとき、アクセス制御ソフトウエア１０は、動作を終了する前に、動作を終了させるべきソフトウエアの名前をユーザ１９０に提示して、提示したソフトウエアの動作を終了してから暗号化ファイル３０を開くよう、ユーザ１９０に通知する。

[0067] ステップＳ６１６において、暗号化ファイル３０に対するファイルアクセス処理を行う。ステップＳ６１６では、ユーザ１９０の操作に応じて行われる復号化ファイルへのアクセス処理を含む。復号化ファイルをクローズする操作をユーザ１９０が行った場合に、制御ソフトウエア１０の動作を終了する。

[0068] 図７は、ユーザ装置１３０における暗号化ファイル３０に対するアクセス処理に関する処理フローの一例である。本処理フローは、図６のステップＳ６１６の処理に適用できる。

[0069] ステップＳ７０２で、アクセス処理部２５０は、管理サーバ１２０に対して、暗号化ファイル３０の復号化用のパスフレーズ６０及び操作制限情報を要求する。具体的には、アクセス処理部２５０は、ユーザ１９０のユーザ識別情報及び暗号化ファイル３０に基づき特定したファイル識別情報とともに、パスフレーズ６０及び操作制限情報を要求する要求情報を管理サーバ１２０に送信する。

[0070] 管理サーバ１２０は、ユーザ装置１３０から受信したユーザ識別情報に基

づいて、ユーザ１９０を認証する。管理サーバ１２０は、ユーザ１９０を認証できた場合、ユーザ装置１３０から受信したユーザ識別情報及びファイル識別情報と、管理サーバ１２０が管理している操作制御情報とに基づいて、ユーザ１９０がアクセス許可者に含まれるか否かを判断する。管理サーバ１２０は、ユーザ１９０がアクセス許可者に含まれると判断した場合に、管理サーバ１２０がファイル識別情報に対応づけて格納しているパスフレーズ６０および操作制限情報を、ユーザ装置１３０に送信する。

[0071] ステップＳ７０４において、アクセス処理部２５０は、暗号化ファイル３０の復号化用のパスフレーズ６０及び操作制限情報を管理サーバ１２０から受信できたか否かを判断する。

[0072] ステップＳ７０４においてアクセス処理部２５０がパスフレーズ６０及び操作制限情報を受信できなかった場合、ステップＳ７２２において、復号化ファイルの情報にアクセスできない旨をユーザ１９０に通知して、ステップＳ７２０において暗号化ファイル３０のクローズ処理を行い、制御ソフトウエア１０の動作を終了する。

[0073] ステップＳ７０４においてアクセス処理部２５０がパスフレーズ６０及び操作制限情報を受信できた場合、ステップＳ７０６において、アクセス処理部２５０は、管理サーバ１２０から受信したパスフレーズ６０を用いて、暗号化ファイル３０を復号化して、復号化ファイル５０を生成する。

[0074] ステップＳ７０８において、動作処理部２４０は、図６のステップＳ６０８またはステップＳ６２２で特定された閲覧ソフトウエアを用いて、復号化ファイル５０を開く。このとき、動作処理部２４０は、管理サーバ１２０から取得した操作制限情報に基づいて、閲覧ソフトウエアを起動させてよい。例えば、動作処理部２４０は、操作制限情報に基づき復号化ファイル５０をネットワーク上へのアップロードを制限する必要があると判断した場合、復号化ファイル５０のアップロードを許可しない動作モードで閲覧ソフトウエアを起動させてよい。

[0075] ステップＳ７１０で、復号化ファイル５０に対する操作を操作制限情報に

基づき制限した状態で、閲覧ソフトウエアに復号化ファイル５０をアクセスさせる。ステップＳ７１０では、復号化ファイル５０へのアクセスに関するユーザ１９０の操作内容を取得する処理、取得した操作内容の操作がユーザ１９０に許可されているか否かを操作制限情報に基づき判断する処理、ユーザ１９０に対して許可された操作に応じた処理だけを閲覧ソフトウエアが行うことを許容する処理等を行う。なお、アクセス処理部２５０は、予め定められた条件に適合する操作があった場合、その操作内容を示す情報を、ユーザ１９０のユーザ識別情報及びファイル識別情報とともに管理サーバ１２０に送信する。管理サーバ１２０は、ユーザ装置１３０から受信したユーザ識別情報及びファイル識別情報に対応づけて、受信した操作内容を示す情報を格納する。係るアクセス制御システム１００の動作によれば、電子ファイル２０のデータに対してユーザ１９０がどのような操作を行ったかを示す操作ログを、電子ファイル２０毎に管理することができる。

[0076] ステップＳ７１２において、動作状態取得部２２０は、現在実行中のプロセスの名前を取得する。具体的には、動作状態取得部２２０は、ステップＳ６１２と同様に、基本ソフトウエアが提供するＡＰＩを通じて、現在実行中のプロセスの名前を取得する。

[0077] ステップＳ７１４において、判断部２１０は、現在実行中のプロセスに基づいて、復号化ファイル５０のデータへのアクセスを保護する必要があるかを判断する。具体的な判断処理は、ステップＳ６１４の処理と同様である。具体的には、判断部２１０は、ステップＳ７１２で取得したプロセスのうちの少なくとも一つのプロセスの名前が、拒否条件のプロセス名に格納されているプロセスの名前のいずれかに一致する場合に、復号化ファイル５０のデータへのアクセスを保護する必要があると判断する。また、判断部２１０は、ステップＳ７１２で取得したプロセスの実行ファイルに、拒否条件の「ＡＰＩ名」に格納されている名前に適合する名前のＡＰＩをコールするコードが含まれている場合に、復号化ファイル５０のデータへのアクセスを保護する必要があると判断する。

[0078] ステップＳ７１４において判断部２１０が復号化ファイル５０のデータへのアクセスを保護する必要がないと判断した場合、ステップＳ７１８に処理を進める。

[0079] ステップＳ７１４において判断部２１０が復号化ファイル５０のデータへのアクセスを保護する必要があると判断した場合、ステップＳ７１６において、動作処理部２４０は、拒否条件に適合するプロセスの動作を終了させる。具体的には、動作処理部２４０は、プロセス名の拒否条件のいずれかに適合する名前を持つプロセスの動作を終了させる。また、動作処理部２４０は、拒否条件の「ＡＰＩ名」に格納されている名前に適合する名前のＡＰＩをコールする実行ファイルに関連するプロセスの動作を終了させる。ステップＳ７１６で拒否条件を満たすプロセスの終了処理が完了すると、ステップＳ７１８に処理を進める。

[0080] ステップＳ７１８で、アクセス処理部２５０は、ユーザ１９０の操作に基づいて、復号化ファイル５０に対するアクセスを終了する指示があった否かを判断する。復号化ファイル５０に対するアクセスを終了する指示がなかった場合は、ステップＳ７１０に処理を戻す。

[0081] ステップＳ７１８で復号化ファイル５０に対するアクセスを終了する指示があったと判断した場合、ステップＳ７２０において、復号化ファイル５０のデータに対するアクセス処理を終了する動作を行う。具体的には、アクセス処理部２５０は、閲覧ソフトウエアが復号化ファイル５０をクローズした後に、復号化ファイル５０を削除する。また、アクセス処理部２５０は、電子ファイル２０のデータへのアクセスを終了した旨を、ユーザ識別情報及びファイル識別情報とともに送信する。電子ファイル２０のデータに対するアクセス処理を終了する処理が完了すると、制御ソフトウエア１０の動作を終了する。

[0082] なお、上述したように、ステップＳ７１４において、判断部２１０は、ステップＳ７１２で取得したプロセスの名前が、拒否条件のプロセス名に格納されているプロセスの名前のいずれかに一致するか否かを判断する。また、

判断部２１０は、ステップＳ７１２で取得したプロセスの実行ファイルが、拒否条件の「ＡＰＩ名」に格納されている名前に適合する名前のＡＰＩをコールするか否かを判断する。ここで、判断部２１０は、ステップＳ７１２で取得したプロセスのうち、ステップＳ６１２で取得したプロセスを除くプロセスを対象として、ステップＳ７１４の判断を行ってよい。このように、判断部２１０は、ステップＳ７１２で取得したプロセスのうち、ステップＳ６１２より後に新たに生成されたプロセスを対象として、上記の判断を行ってよい。また、判断部２１０は、ステップＳ７１４の判断を、直前の判断より後に新たに生成されたプロセスを対象として行ってよい。

[0083] なお、ステップＳ６１２の処理及びステップＳ６１４の処理は、暗号化ファイル３０にアクセスするアクセス処理用の実行単位とは異なるプロセス監視用の実行単位で行ってよい。プロセス監視用の実行単位は、ステップＳ６１２の処理及びステップＳ６１４の処理を定期的に行ってよい。例えば、ステップＳ６１２の処理及びステップＳ６１４の処理は、アクセス処理用のプロセスとは異なる、プロセス監視用のプロセスで行ってよい。また、ステップＳ６１２の処理及びステップＳ６１４の処理は、アクセス処理用のスレッドとは異なる、プロセス監視用のスレッドで行ってよい。そして、アクセス処理用の実行単位は、例えばステップＳ６１２及びステップＳ６１４の処理に代えて、プロセス監視用の実行単位からステップＳ６１４の判断結果を示す情報を取得して、プロセス監視用の実行単位から取得した情報が示す判断結果に基づいて、ステップＳ６４２及びステップＳ６１６のいずれに進むかを判断してよい。同様に、アクセス処理用の実行単位は、ステップＳ７１２及びステップＳ７１４の処理に代えて、プロセス監視用の実行単位からステップＳ７１４の判断結果を示す情報を取得して、ステップＳ７１６の処理を行うか否かを判断してよい。なお、プロセス監視用の実行単位が、ステップＳ７１６の処理を行ってよい。この場合、アクセス用の実行単位は、プロセス監視用の実行単位に、拒否条件に適合するプロセスの動作を終了させる処理を依頼してよい。これに代えて、プロセス監視用の実行単位は、アクセス

用の実行単位がステップＳ７１６以降の処理を行っている間、ステップＳ６１４の判断結果に応じて、拒否条件に適合するプロセスの動作を終了させてよい。

[0084] また、制御ソフトウエア１０の動作によってユーザ装置１３０で行われるステップＳ６１０の判断処理、ステップＳ６１４の判断処理及びステップＳ７１４の判断処理のうち少なくとも一つの判断処理を、ユーザ装置１３０の代わりに管理サーバ１２０が行ってもよい。そして、ユーザ装置１３０は、管理サーバ１２０によって行われた判断処理の結果を示す情報を、管理サーバ１２０から取得してよい。この場合、ユーザ装置１３０は、これらの判断処理を行うために管理サーバ１２０が必要とする情報を、管理サーバ１２０に送信してよい。例えば、ユーザ装置１３０は、ステップＳ６０８またはステップＳ６２２で特定した閲覧ソフトウエアの名前を示す情報を、管理サーバ１２０に送信してよい。また、ユーザ装置１３０は、ステップＳ６１２またはステップＳ７１２で特定したプロセスの名前を示す情報を、管理サーバ１２０に送信してよい。これにより、ユーザ装置１３０は、管理サーバ１２０で管理されている最新の許可条件及び拒否条件に基づいて、暗号化ファイル３０に対するアクセスを制御することができる。

[0085] なお、許可条件は、ソフトウエアに関するいわゆるホワイトリストに相当するとみなせる。また、拒否条件は、ソフトウエアに関するいわゆるブラックリストに相当するとみなせる。そのため、アクセス制御システム１００によれば、ソフトウエアに関するホワイトリスト及びブラックリストに基づいて、電子ファイル２０のデータに対するアクセスを制御することができるといえる。

[0086] なお、暗号化ファイルは、電子ファイルの一例である。本実施形態では、暗号化ファイルに対するアクセス処理を取り上げて説明した。しかし、本実施形態に関して説明したアクセス制限処理は、暗号化ファイルに限られず、暗号化されていない電子ファイルを対象に適用し得る。また、本実施形態に関して説明したアクセス制限処理は、電子ファイルのデータに限られず、種

々のデータまたは情報を対象に適用し得る。

[0087] 上記の説明において、制御部２００の動作として説明した処理は、プロセッサが制御ソフトウエア１０及び基本ソフトウエア等のプログラムに従ってユーザ装置１３０が有する各ハードウェアを制御することにより実現される。すなわち、本実施形態のユーザ装置１３０に関連して説明したユーザ装置１３０の処理は、プロセッサがプログラムに従って動作して各ハードウェアを制御することにより、プロセッサ、メモリ等を含む各ハードウェアとプログラムとが協働して動作することにより実現することができる。すなわち、当該処理を、いわゆるコンピュータで実現することができる。コンピュータは、上述した処理の実行を制御するプログラムをロードして、読み込んだプログラムに従って動作して、当該処理を実行してよい。コンピュータは、当該プログラムを記憶しているコンピュータ読取可能な記録媒体から当該プログラムをロードすることができる。

[0088] 以上、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記実施の形態に記載の範囲には限定されない。上記実施の形態に、多様な変更または改良を加えることが可能であることが当業者に明らかである。その様な変更または改良を加えた形態も本発明の技術的範囲に含まれ得ることが、請求の範囲の記載から明らかである。

[0089] 請求の範囲、明細書、及び図面中において示した装置、システム、プログラム、及び方法における動作、手順、ステップ、及び段階等の各処理の実行順序は、特段「より前に」、「先立って」等と明示しておらず、また、前の処理の出力を後の処理で用いるのでない限り、任意の順序で実現しうることに留意すべきである。請求の範囲、明細書、及び図面中の動作フローに関して、便宜上「まず、」、「次に、」等を用いて説明したとしても、この順で実施することが必須であることを意味するものではない。

符号の説明

[0090] １０ 制御ソフトウエア

２０ 電子ファイル

３０　暗号化ファイル

５０　復号化ファイル

６０　パスフレーズ

７０　電子メール

８０　記録メディア

９０　通信ネットワーク

１００　アクセス制御システム

１１０　ユーザ装置

１２０　管理サーバ

１３０　ユーザ装置

１８０　ユーザ

１９０　ユーザ

２００　制御部

２０２　送受信部

２０４　格納部

２１０　判断部

２２０　動作状態取得部

２３０　ソフトウエア特定部

２４０　動作処理部

２５０　アクセス処理部

請求の範囲

[請求項1] 電子ファイルのアクセスが許可または禁止されているソフトウエアが予め定められたアクセス制御情報に基づいて電子ファイルへアクセスすることを制限する制御部
を備えるアクセス制御装置。

[請求項2] 前記アクセス制御情報は、前記アクセスに用いることが許可されるソフトウエアが満たすべき予め定められた第１条件を含み、
前記制御部は、前記電子ファイルのアクセスに用いるべきソフトウエアが前記第１条件を満たす場合に、前記第１条件を満たすソフトウエアによる前記アクセスを許可する
請求項１に記載のアクセス制御装置。

[請求項3] 前記アクセス制御情報は、前記アクセスが禁止されるソフトウエアが満たすべき予め定められた第２条件を含み、
前記制御部は、前記第２条件を満たすソフトウエアによる前記アクセスを制限する
請求項２に記載のアクセス制御装置。

[請求項4] 前記制御部は、前記第２条件を満たすソフトウエアが動作している場合に、前記第１条件を満たすソフトウエアによる前記アクセスを制限する
請求項３に記載のアクセス制御装置。

[請求項5] 前記制御部は、前記第１条件を満たすソフトウエアが前記電子ファイルへのアクセスを開始する前に、前記第２条件を満たすソフトウエアが動作しているか否かを判断し、前記第２条件を満たすソフトウエアが動作していると判断した場合に、前記第１条件を満たすソフトウエアが前記電子ファイルへのアクセスを開始することを禁止する
請求項４に記載のアクセス制御装置。

[請求項6] 前記制御部は、前記第１条件を満たすソフトウエアが前記電子ファイルへのアクセスを開始した後に、前記第２条件を満たすソフトウエ

アの動作が検出された場合に、前記第２条件を満たすソフトウエアの動作を制限する

請求項５に記載のアクセス制御装置。

[請求項7] 前記第２条件は、前記アクセスが禁止されるべきソフトウエアが行う動作内容に関する条件を含む

請求項３から６のいずれか一項に記載のアクセス制御装置。

[請求項8] 暗号化された電子ファイルの復号化に用いるパスフレーズを外部の管理装置から取得するパスフレーズ取得部と、

前記パスフレーズ取得部が取得した前記パスフレーズを用いて、前記暗号化された電子ファイルを復号化する復号化部と

をさらに備え、

前記制御部は、前記復号化部が前記暗号化された電子ファイルを復号化する前に、前記復号化部により復号化された電子ファイルへのアクセスを許可するか否かを前記予め定められたアクセス制御情報に基づいて判断し、前記復号化部により復号化された電子ファイルへのアクセスを許可すると判断した場合に、前記パスフレーズ取得部に前記管理装置から前記パスフレーズを取得させ、前記暗号化された電子ファイルを前記復号化部に前記パスフレーズを用いて復号化させる

請求項２から７のいずれか一項に記載のアクセス制御装置。

[請求項9] コンピュータを、請求項１から８のいずれか一項に記載のアクセス制御装置として機能させるためのプログラム。

[請求項10] 請求項１から８のいずれか一項に記載のアクセス制御装置と、

前記アクセス制御装置の外部に設けられ、前記予め定められたアクセス制御情報及び前記予め定められたアクセス制御情報に基づく判断結果の少なくとも一方を、前記アクセス制御装置に提供する管理装置と

を備えるアクセス制御システム。